Section II:	**Administrative Security**
Title:	**Data Stewardship Security Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**June 11, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To ensure that the North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices appropriately secure, safeguard, and handle DHHS data and/or information.

STANDARD

1.0 Background

The Divisions and Offices management, with the assistance from the Division Information Security Official (ISO), shall ensure that information security is effectively implemented by designating proper workforce member security roles and responsibilities. In addition, the Divisions and Offices must establish their own policies, procedures, standards, and guidelines as defined in this standard.

2.0 Recording Data Stewards and Data System Owners

No one individual within the Divisions and Offices owns Division and Office data and/or information. The Division ISO or designee shall be responsible for creating a list of all Data Stewards, as assigned by Data Owner. In addition, the Division ISO shall maintain a record of all DHHS System Owners that have authorization and access controls to DHHS data and/or information. In order to ensure a proper list of Data Stewards and DHHS System Owners are maintained, the Division ISO shall monitor their records periodically to ensure that changes are updated accordingly.

3.0 Naming and Defining Data and/or Information

The Division ISO shall assist Data Stewards with naming and defining the data and/or information that is owned by DHHS. When data is created and owned by third-party vendors, it must be defined based on the third-party owner's contract guidelines and service level agreements (SLAs).

All Data Stewards must ensure that proper records are kept once data is named and defined in order to ensure that the data and/or information are not misrepresented across DHHS. It is imperative that the Division ISOs and the Data Stewards ensure the named and defined data is secured, safeguarded, and maintained. This process must include the workforce members or approved/authorized third-party vendors doing data backup and storage. All DHHS data and/or information being backed-up and stored must be properly secured, safeguarded, and maintained in order to reduce malicious tampering.

4.0 Stored Data and/or Information

All Divisions and Offices management, with the assistance from the Division ISO, shall ensure that stored data and/or information shall be readily available to appropriate DHHS workforce members except when access restrictions have been determined appropriate and applicable. All Division and Office management must ensure that guideline restrictions are created, enforced, monitored, and followed.

5.0 Handling and Labeling Data and/or Information

DHHS confidential data and/or information shall be labeled to reflect its current classification status. All data and/or information must be clearly labeled regardless of the type of storage media device or classification status.

The Divisions and Offices Data Stewards, System Owners, and Data Users must ensure that data and/or information be handled in an appropriate manner that will reduce the risk of accidental disclosure, modification, or loss. The handling of data and/or information will depend on the following functions:

- Nature of the operating environment
- The potential exposures
- The unauthorized access to or modification of the data

All Division and Office data and/or information must be handled and stored in accordance with the NC DHHS Security Standards, Administrative Security Standards – Information Classification Security Standard.

A Division or Office that uses protected information from another Division or Office shall observe, secure, safeguard, and maintain the confidentiality conditions imposed by the granting Division and Office.

An appropriate set of procedures should be defined for handling information in accordance with the NC DHHS Security Standards, Administrative Security Standards – Information Classification Security Standard. The procedures should cover data and/or information assets in both physical and electronic formats. For each classification, the handling procedures should be defined to cover the following types of information processing activities:

- Copying
- Backups
- Storing
- Transmitting by post, fax, and electronic mail
- Transmitting by spoken word (e.g., mobile phone and voice mail)
- Answering machines

The output from systems containing data and/or information that are classified as confidential should carry an appropriate classification label. The labeling should reflect the classification according to the rules established in Section 2.0: Classifying DHHS Information, of the NC DHHS Security Standards,

Administrative Security Standards – Information Classification Security Standard. Other items for consideration may include printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, cassettes, USB flash memory drives, etc.), electronic messages, and file transfers.

All DHHS physical assets that contain confidential data and/or information must be labeled and marked according to the naming and defining guidelines listed in this standard. Physical labels are generally the most appropriate forms of labeling; however, some data and/or information, such as documents in electronic form, cannot be physically labeled and electronic means of labeling need to be used.

When transmitting telecommunication messages (e.g., telephone calls, telex/cables, facsimiles, emails, computer transactions, etc.), it is imperative that the originator does not compromise the confidentiality, integrity, or availability of data and/or information being transmitted.

6.0 Determining Data Stewardship Security Roles and Responsibilities

The Divisions and Offices management, with the assistance from Division ISO, shall determine the data stewardship and Data User security roles and responsibilities, prior to posting job qualifications. All data stewardship and Data User security duties shall be included in the job vacancy list. In addition, the DHHS Division and Office management must notify Data Stewards and Data Users when security duties change to ensure job roles and responsibilities are carried out appropriately.

Reference:

- HIPAA Administration Simplification Act - 45 C.F.R. Parts 160 and 164.
  - HIPAA – 45 C.F.R. § 164.308(a)(1) Security Management Process.
  - HIPAA – 45 C.F.R. § 164.308(a)(2) Assigned Security Responsibility.
  - HIPAA – 45 C.F.R. § 164.308(a)(3) Workforce Security.
  - HIPAA – 45 C.F.R. § 164.308(a)(7) Contingency Plan.
  - HIPAA – 45 C.F.R. § 164.308(a)(7)(ii)(A) Data Backup Plan.
  - HIPAA – 45 C.F.R. § 164.308(a)(7)(ii)(C) Emergency Mode Operation Plan.
  - HIPAA – 45 C.F.R. § 164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis.
  - HIPAA – 45 C.F.R. § 164.310(d)(1) Device and Media Controls.
  - HIPAA – 45 C.F.R. § 164.310(d)(2)(iv) Data Backup and Storage.
  - HIPAA – 45 C.F.R. § 164.312(a)(1) Access Control.
  - HIPAA – 45 C.F.R. § 164.312(a)(2)(ii) Emergency Access Procedure.
  - HIPAA – 45 C.F.R. § 164.312(b) Audit Controls.
  - HIPAA – 45 C.F.R. § 164.312(c)(1) Integrity.
  - HIPAA – 45 C.F.R. § 164.312(e)(1) Transmission Security.
  - HIPAA – 45 C.F.R. § 164.314(a)(1) Business Associate Contracts or Other Agreements.

- NC Statewide Information Security Manual
  - Statewide IT Policies and Standards
    - Other Security Standards and Procedures
      - Confidential Information Policy

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Classification Security Standard
    - Information Security Change Management Standard
    - Information Security Risk Management Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Information Systems Review and Auditing Policy